U.S. Department of Homeland Security

United States Secret Service

PRESS RELEASE

August 25, 2016
Contact: (202) 406-5708
GPA 15 - 16

RUSSIAN CYBER-CRIMINAL CONVICTED OF 38-COUNT INDICTMENT FOLLOWING 10-YEAR SECRET SERVICE INVESTIGATION

Hacking Scheme Involving Millions of Credit Card Numbers Defrauded Banks of More Than $169 Million

Seattle, WA – A federal court jury today convicted Roman Valerevich Seleznev, aka "Track2," 32, of Vladivostok, Russia, of 38 counts related to his scheme to hack into point-of-sale computers to steal and sell credit card numbers to the criminal underworld. This conviction follows a 10-year investigation by U.S. Secret Service personnel around the globe.

The jury deliberated six hours following an eight-day trial. U.S. District Judge Richard A. Jones scheduled sentencing for December 2, 2016.

The 40-count indictment charged Seleznev with the theft and sale of more than 2 million credit card numbers. According to testimony at trial and court documents, the Secret Service first began tracking the activities of Seleznev in 2005. He was alleged to be one of the senior members of several organized online criminal networks. Between October 2009 and October 2013, Seleznev hacked into retail point-of-sale systems and installed malicious software to steal credit card numbers from various businesses.

Seleznev operated a server in Russia that he used to install malware on the point-of-sale computer systems. The malware would steal the credit card data from the point-of-sale systems and send it to other servers controlled by Seleznev in the Ukraine or in McLean, Virginia. Seleznev would bundle the credit card information into groups called "bases" and sell the information on various "carding" websites. The buyers would then use the credit card numbers for fraudulent purchases. Testimony at trial revealed that 3,700 financial institutions lost more than $169 million because of the scheme.

When Seleznev was taken into custody by Secret Service agents in July 2014 in the Maldives, his laptop contained more than 1.7 million stolen credit card numbers. Also on the laptop was additional evidence linking Seleznev to the servers, email accounts and financial transactions involved in the scheme.

In closing arguments prosecutors told the jury to "follow the digital fingerprints" that Seleznev left across the internet and they would find "one of the most prolific credit card thieves in history."

Seleznev was convicted of ten counts of wire fraud, eight counts of intentional damage to a protected computer, nine counts of obtaining information from a protected computer, nine counts of possession of 15 or more unauthorized access devices and two counts of aggravated identity theft. Wire fraud is punishable by up to thirty years in prison and a $1 million fine. Intentionally causing damage to a protected computer resulting with a loss of more than $5,000 is punishable by up to ten years in prison and a $250,000 fine. Obtaining information from a protected computer is punishable by up to five years in prison and a $250,000 fine. Possession of more than 15 unauthorized access devices is punishable by up to ten years in prison and a $250,000 fine. Aggravated identity theft is punishable by an additional two years in prison on top of any sentence for the underlying crimes. In determining the actual sentence, the Court will consider the United States Sentencing Guidelines, which are not binding but provide appropriate sentencing ranges for most offenders.

Seleznev is also charged in a separate indictment in the District of Nevada with participating in a racketeer influenced corrupt organization (RICO) and conspiracy to engage in a racketeer influenced corrupt organization, as well as two counts of possession of 15 or more counterfeit and unauthorized access devices. This indictment is the result of the Secret Service's Las Vegas Field Office investigation "Operation Open Market" involving 50 suspects associated with the "Carder.su" criminal organization. Seleznev is also charged in the Northern District of Georgia with conspiracy to commit bank fraud, one count of bank fraud, and four counts of wire fraud.

The Seattle case was investigated by the U.S. Secret Service Electronic Crimes Task Force, which includes detectives from the Seattle Police Department and the U.S. Secret Service Cyber Intelligence Section in Washington DC. The case is being prosecuted by Assistant U.S. Attorneys of the Western District of Washington and the Criminal Division's Computer Crime and Intellectual Property Section.

About the United States Secret Service

The United States Secret Service was originally founded in 1865 for the purpose of suppressing the counterfeiting of U.S. currency. Now an agency within the Department of Homeland Security, the Secret Service is widely known for its protective mission in safeguarding the nation's highest elected officials, visiting foreign dignitaries and events of national significance. Today, the Secret Service maintains a unique integrated mission of protection and investigations, as one of the premier law enforcement organizations charged with investigating cyber and financial crimes.

# # #

EDITOR'S NOTE: For questions concerning this release, please contact the U.S. Secret Service Office of Government and Public Affairs at 202-406-5708.